Gustavo Ponce, Esq.
Nevada Bar No. 15084
Mona Amini, Esq.
Nevada Bar No. 15381
KAZEROUNI LAW GROUP, APC
6787 W. Tropicana Avenue, Suite 250
Las Vegas, Nevada 89103
Telephone: (800) 400-6808
Facsimile: (800) 520-5523
E-mail: mona@kazlg.com
Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

HEATHER HILLBOM, individually and on behalf of all others similarly situated, Plaintiff, vs. R1 RCM, INC.; and DIGNITY HEALTH d/b/a DIGNITY HEALTH - ST. ROSE DOMINICAN HOSPITAL, ROSE DE LIMA CAMPUS, Defendants.	Case No.: **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

//

//

//

//

//

//

//

//

INTRODUCTION

1. Plaintiff Heather Hillbom ("Plaintiff"), individually and on behalf of all others similarly situated (collectively, the "Class members") brings this class action against Defendants R1 RCM, Inc. ("R1") and Dignity Health d/b/a St. Rose Dominican Hospital, Rose de Lima Campus ("Dignity") (jointly as "Defendants"), for their failure to secure and safeguard Plaintiff's and approximately 16,120 similarly situated Class members' personally identifying information ("PII") and personal health information ("PHI"), including but not limited to their names, Social Security numbers, dates of birth, addresses, contact information, medical record numbers, patient account numbers, medical information, and location of services.

2. R1 is a third-party vendor of technology-based revenue cycle management services for hospitals, health systems, physician groups, and other entities in the healthcare industry.

3. Sometime between January 30, 2023, and November 17, 2023, an unauthorized third party gained access to R1's network system and obtained files containing information about Dignity's current and former patients, including Plaintiff and the Class (the "Data Breach").

4. Defendants owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access, disclosure, and exfiltration by unauthorized third parties. Defendants breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect Plaintiff and other similarly situated Dignity patients' PII/PHI from unauthorized access and disclosure.

5. As a result of Defendants' inadequate data security and breach of their duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed, disclosed, viewed, and exfiltrated by unauthorized third parties that took possession of Plaintiff's and the Class members' PII/PHI. Further, Plaintiff and the Class (defined below) have been placed in an imminent and continuing risk of harm from fraud, identity theft, and related harm caused by the Data Breach and should remain vigilant for any signs of fraud or identity theft for the indefinite future.

6. As a result of Defendant's conduct, Plaintiff and the Class have and will be required to continue to undertake time-consuming and often costly efforts to mitigate the actual and potential harm caused by the Data Breach. This includes efforts to mitigate the breach's exposure of their PII, including by, among other things, placing freezes and setting alerts with credit reporting agencies, contacting financial institutions, closing, or modifying financial accounts, reviewing, and monitoring credit reports and accounts for unauthorized activity, changing passwords on potentially impacted websites and applications, and requesting and maintaining accurate records.

7. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all persons whose privacy and PII/PHI was impacted by the Data Breach, which occurred sometime between January 30, 2023, and November 17, 2023.

8. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, including negligence per se, breach of implied contract, unjust enrichment, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

JURISDICTION AND VENUE

9. This Court has subject matter of this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, and there are more than 100 members in the proposed Class, and at least one member of the Class is a citizen of a state different from Defendants.

10. This Court has personal jurisdiction over Defendant R1 because it is a corporation that regularly transacts business within this state, has a registered agent in this state, and makes or performs contracts within this state, including its business association and contracts with Defendant Dignity Health.

11. This Court has personal jurisdiction over Defendant Dignity Health because it operates several Dignity hospitals within this state, including the St. Rose Dominican Hospital, Rose de Lima Campus within this state, and this judicial district.

12. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391(a) and (b) because a substantial part events and injury giving rise to Plaintiff's claims occurred in or originated

from this District and Defendant does business and transact business in this judicial district.

PARTIES

13. Plaintiff is a citizen and resident of the State of Nevada and in this judicial district.

14. Sometime prior to the Data Breach, Plaintiff was a patient of and obtained healthcare or related services from Dignity, including at its St. Rose Dominican Hospital, Rose de Lima Campus located in Henderson, Nevada. As a condition of receiving services, Dignity required Plaintiff to provide them with her PII/PHI.

15. Based on representations made by Dignity, and Plaintiff's reliance on such representations, Plaintiff believed Dignity had implemented and maintained reasonable security and practices to protect her PII/PHI from unauthorized access. Relying on Dignity's representations and her belief that her PII/PHI would be reasonably safeguarded, Plaintiff provided her PII/PHI to Dignity in connection with receiving healthcare services. Plaintiff's PII/PHI was entrusted to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with its obligations to keep such information confidential and secure from unauthorized access.

16. Plaintiff takes great care to protect her PII/PHI. If Plaintiff had known that Dignity would not adequately protect the PII/PHI in its possession, including by contracting with companies that do not adequately protect the PII/PHI in their possession, she would not have agreed to entrust Dignity with her PII/PHI or obtained healthcare services from Dignity.

17. Plaintiff received a letter from Defendants, dated March 11, 2024, informing Plaintiff, in relevant portion, of the following:

> R1 RCM Inc. ("R1") is providing this notice to you on behalf of St. Rose Dominican Hospital de Lima, a Dignity Health hospital ("Dignity") regarding an incident that may have impacted the privacy of your protected health information ("PHI"). R1 is contacting you because we are a business associate of Dignity and processed your PHI in the course of providing those services. This notice provides information about the incident, the actions we are taking out of an abundance of caution and what to do if you have further questions."
>
> R1 became aware on November 17, 2023 that PHI associated with Dignity was in the possession of an unauthorized third party (the "Dignity PHI"). R1 immediately began an investigation into the matter and determined a copy of this PHI was present on a server maintained by CloudMed, an R1 company, when the server was targeted by the exploitation of a zero-day

> vulnerability of GoAnywhere software by the same unauthorized third party on January 30, 2023 (the "GoAnywhere Event"). While we could not definitively confirm that the GoAnywhere Event was the source of the PHI at issue, we are nonetheless providing this notice out of an abundance of caution.
>
> R1 undertook an analysis of the Dignity PHI and on, January 11, 2024, determined that certain PHI, including your name, contact information, date of birth, Social Security number, location of services, clinical and/or diagnosis information and patient account and/or medical record number was potentially included in the Dignity PHI.
>
> In connection with R1's response to the GoAnywhere Event, R1 rebuilt the impacted server and implemented the patch released by GoAnywhere in February 2023 designed to address the vulnerability at issue. In addition, out of an abundance of caution, we have secured the services of Kroll to provide two years of identity monitoring services at no cost to you.

18. Since learning of the Data Breach, Plaintiff has undertaken reasonable efforts to mitigate the impact of the Data Breach, including but not limited to reviewing her accounts and credit reports for any indications of fraud or identity theft, freezing her credit, and replacing debit or cards. As a result of the Data Breach, Plaintiff will continue to spend valuable time for the remainder of her life, to mitigate the impact of the Data Breach, and dispute and rectify the fraud and/or damage to her credit reputation experienced as a result of the Data Breach which Plaintiff otherwise would have spent on other activities, including but not limited to leisure, work, and/or recreation.

19. Since the Data Breach, Plaintiff has noticed unauthorized credit inquiries on her credit report, and learned that her PII were found on the dark web, which Plaintiff believes to be attributed to the Data Breach. In addition, Plaintiff has spent time and incurred costs enrolling in credit monitoring and identity theft protection services in order to further mitigate the impact of the Data Breach.

20. As a direct result of the Data Breach, Plaintiff has suffered injury and damages including, *inter alia*, invasion of privacy, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security. Plaintiff and the Class has incurred and will continue to incur this damage in addition to any fraudulent use of their sensitive personal information, including their PII/PHI, for

years to come.

21. Defendant R1 is a Delaware corporation with a corporate headquarters or principal place of business at 433 W. Ascension Way Suite 200, Murray, Utah 84123.

22. Defendant Dignity Health is headquartered in San Francisco, California, and operates numerous hospitals, including St. Rose Dominican Hospital, Rose de Lima Campus located in Henderson, Nevada.

FACTUAL ALLEGATIONS

PII/PHI Is a Valuable Property Right that Must Be Protected

23. In a Federal Trade Commission ("FTC") roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored the property value attributed to PII by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[1]

24. The value of PII as a commodity is measurable. "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[2] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" for several years.

25. Companies recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[3]

26. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals openly post credit card numbers, Social Security numbers, PII and other sensitive information directly on various illicit Internet websites making the information publicly

---

[1] FTC, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

[2] *See* Soma, *Corporate Privacy Trend, supra*.

[3] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

available for other criminals to take and use. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list."

27. Recognizing the high value that consumers place on their PII, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share – and who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the surrender of their PII.[4] This business has created a new market for the sale and purchase of this valuable data.[5]

28. Consumers place a high value not only on their PII, but also on the privacy of that data. Researchers shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[6]

29. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII between $11.33 and $16.58 per website.[7]

30. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[4] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010) *available at* https://www.nytimes.com/2010/07/18/business/ 18unboxed.html.

[5] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011) *available at* https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

[6] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), *available at* https://www.jstor.org/stable/23015560?seq=1#

[7] II–Horn, Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at* https://ideas.repec.org/p/wpa/wuwpio/0304001.html (emphasis added).

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

31. A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. As more consumers rely on the internet and apps on their phone and other devices to conduct every-day transactions, data breaches are becoming increasingly more harmful.

32. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a person's name.[8] As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

33. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records … [and their] good name." According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[9]

34. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[10] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[11]

---

[8] *See* GAO, GAO Report 9 (2007) *available at* http:///www.gao.gov/new.items/d07737.pdf.

[9] *See* FTC Identity Theft Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

[10] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer, or taxpayer identification number." *Id.*

[11] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), *available at*

35. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[12]

36. According to the IBM and Ponemon Institute's 2019 "Cost of a Data Breach" report, the average cost of a data breach per consumer was $150 per record.[13] Other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft – a common result of data breaches – was $298 dollars.[14] And in 2019, Javelin Strategy & Research compiled consumer complaints from the FTC and indicated that the median out-of-pocket cost to consumers for identity theft was $375.[15]

37. A person whose PII has been compromised may not see any signs of identity theft for years. According to the GAO Report:

> "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."

---

https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[12] Brian Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying- about-identity-theft.

[13] Brook, *What's the Cost of a Data Breach in 2019*, *supra*.

[14] Norton By Symantec, 2013 Norton Report 8 (2013), *available at* https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf.

[15] Facts + Statistics: *Identity Theft and Cybercrime*, Insurance Information Institute, *available at* https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (citing the Javelin report).

38. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.[16]

39. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[17] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[18]

40. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[19]

41. According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[20]

42. It is within this context that Plaintiff and thousands of similar individuals must now live with the knowledge that their PII/PHI is forever in cyberspace, putting them at imminent and continuing risk of damages, and was taken by unauthorized persons willing to use the information for any number of improper purposes and scams, including making the information available for sale on the dark web and/or the black market.

Defendants and their Collection of PII/PHI

43. Upon information and belief, R1 is "a business associate of Dignity and processed [Plaintiff's] PHI in the course of providing those services" to Dignity.[21]

---

[16] *See* Cory Scott, *Protecting Our Members*, LINKEDIN (May 18, 2016), *available at* https://blog.linkedin.com/2016/05/18/protecting-our-members.
[17] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAG. (Oct. 20, 2019) https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon
[18] *Id.*
[19] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices- in-the-online-black-market.
[20] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[21] https://www.mass.gov/doc/assigned-data-breach-number-2024-477-r1-rcm-inc/download

44. Upon information and belief, Dignity used R1 for revenue cycle management services.[22]

45. Plaintiff and Class members are current or former patients of Dignity and entrusted Dignity with their PII/PHI, including but not limited to the PII/PHI compromised by the Data Breach.

The Data Breach

46. Between approximately January 30, 2023, and November 17, 2023, "an unauthorized third party" gained access to "protected health information ("PHI") associated with Dignity."[23]

47. According to the Notice of Cybersecurity Incident posted on Dignity's website,[24] the PII/PHI affected in the Data Breach compromised the patient name, contact information, date of birth, location of services, clinical and/or diagnosis information, patient account and/or medical record number, and Social Security number, of Plaintiff and the Class members.

48. Defendants reported to the U.S. Department of Health and Human Services' Office for Civil Rights that on "3/11/2024," R1 reported an "Hacking/IT Incident" involving a "Network Server" affecting "16121" individuals.

49. Dignity's Notice of Privacy Practices states, "We understand that your protected health information is private and personal. We are committed to protecting it…We are required by law to keep your protected health information private…[and] notify you as outlined in state and federal law if a breach of your unsecured protected health information has occurred."[25]

50. R1 became aware of the data breach on November 17, 2023; and, based on Defendants' data breach notice letter, the Data Breach occurred as early as January 30, 2023. Thus, it is possible that it took over nine (9) months for Defendants to even realize the Data Breach occurred. However, Defendants failed to notify Plaintiff and the Class members until on or around March 11, 2024, almost four (4) months after their knowledge of the Data Breach.

---

[22] https://www.dignityhealth.org/las-vegas/website-notice/r1-provides-notice-of-cybersecurity-incident

[23] *Id.*

[24] *Id.*

[25] https://www.dignityhealth.org/content/dam/dignity-health/pdfs/hipaa-notices-of-privacy-practices/Notice%20of%20Privacy%20Practices%20DH%20NV%2010.2020.pdf

51. Defendants' failure to both promptly discover and notify Plaintiff and Class members that their PII/PHI was accessed and stolen by unauthorized third parties allowed those who were able to obtain their PII/PHI to monetize, misuse, or disseminate that PII/PHI before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and the Class members have and will continue to suffer indefinitely from the damage of substantial, imminent, and concrete risk that their identities will be, or already have been, stolen and misused by unauthorized third parties.

52. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities to provide notification following a breach of unsecured protected health information. Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals. Covered entities must *only* provide the required notifications if the breach involved unsecured protected health information. Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of the U.S. Dept. of Health and Human Services in guidance. Under approved guidance of the U.S. Dept. of Health and Human Services, protected health information ("PHI") is rendered unusable, unreadable, or indecipherable to unauthorized individuals if (1) electronic PHI has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption) and (2) such confidential process or key that might enable decryption has not been breached. By reporting this incident to the U.S. Dept. of Health and Human Services, by sending its data breach notification letter, Defendants have determined and affirmed that Plaintiff's and the Class Members' electronic PII/PHI was either not encrypted at all, or if it was encrypted, the encryption has been breached by the unauthorized third party. As a result, Defendants were negligent for failing to encrypt or adequately encrypt Plaintiff's and the Class Members' electronic medical information.

53. Plaintiff's and Class Members' unencrypted PII/PHI may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII and PHI of Plaintiff and Class Members.

54. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing their PII and PHI to be exposed, accessed, disclosed, viewed, and taken by unauthorized parties.

55. As a condition of its relationships with Plaintiff and Class Members, Defendants required that Plaintiff and Class Members entrust Defendants with highly confidential PII and PHI.

56. By obtaining, collecting, and storing the PII and PHI of Plaintiff and Class Members, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII and PHI from unauthorized access, disclosure, viewing, and exfiltration.

57. Plaintiff and Class Members took reasonable steps to maintain the confidentiality of their PII and PHI and relied on Defendants to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of such sensitive and private personal information.

58. Defendants could have prevented this Data Breach by properly safeguarding and encrypting the PII and PHI of Plaintiff and Class Members. In addition, to the extent permissible, Defendants could have destroyed the data, especially old data from former patients.

59. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII and PHI of Plaintiff and Class Members from being compromised in the Data Breach.

60. As a result of the Data Breach and Defendants' conduct and/or omissions, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the unauthorized disclosure and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery

from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for services that were received without adequate data security to reasonably safeguard Plaintiff and the Class members' PII/PHI from unauthorized disclosure, access, and exfiltration.

CLASS ACTION ALLEGATIONS

61. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff seeks to represent and intends to seek certification of a class (the "Class") defined as:

> **All individuals whose PII/PHI was impacted by the Data Breach, including all individuals who were sent a notice of the Data Breach by or on behalf of Defendants**.

62. Excluded from the Class are: (1) Defendants and their respective officers, directors, employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

63. Certification of Plaintiff's claims for class wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

64. Plaintiff reserves the right to, after conducting discovery, modify, expand, or amend the above Class definition or to seek certification of a class or Classes defined differently than above before any court determines whether certification is appropriate.

65. The Class members are so numerous and geographically dispersed throughout California that joinder of all Class members would be impracticable. While the exact number of Class members is unknown, based on information and belief, the Class consists of tens of thousands of individuals, including Plaintiff and the Class members. Plaintiff therefore believe that the Class is

so numerous that joinder of all members is impractical.

66. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had their PII compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

67. There is a well-defined community of interest in the common questions of law and fact affecting Class members. The questions of law and fact common to Class members predominate over questions affecting only individual Class members, and include without limitation:

a) Whether Defendants had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII/PHI it collected, stored, and maintained from Plaintiff and Class members;

b) Whether Defendants had duties not to disclose the PII/PHI of Plaintiff and Class members to unauthorized third parties;

c) Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII/PHI;

d) Whether Defendants breached their duty to protect the PII/PHI of Plaintiff and each Class member; and

e) Whether Plaintiff and each Class member are entitled to damages and other equitable relief.

68. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that Plaintiff has no interests adverse to or that conflicts with the Class Plaintiff seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection and consumer privacy class actions of this nature.

69. A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class members is impractical.

Furthermore, the expenses and burden of individual litigation would make it difficult or impossible for the individual members of the Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class are outweighed by the costs of suit. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

70. Defendants have acted or refused to act on grounds generally applicable to the entire Class, thereby making it appropriate for this Court to grant final injunctive, including public injunctive relief, and declaratory relief with respect to the Class as a whole.

CAUSES OF ACTION

COUNT I

NEGLIGENCE

71. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

72. Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting the PII/PHI in their possession, custody, or control.

73. In addition, Defendants' duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules"). Defendants' duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Defendants, of failing to employ reasonable measures to protect and secure Plaintiff and the Class members' PII/PHI.

74. Defendants' violation of the HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence *per se*.

75. Defendants knew or should have known the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. Defendants knew or should have known of the many data breaches that targeted healthcare provides that collect and store PII/PHI in recent years.

76. Given the nature of Defendants' businesses, the sensitivity and value of the PII/PHI they maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities to their systems or their third-party vendor's systems and prevented the Data Breach from occurring.

77. Defendants breached these duties by failing to, or contracting with companies that failed to, exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

78. It was reasonably foreseeable for Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

79. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be

required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security measures implemented by Defendants.

COUNT II

BREACH OF IMPLIED CONTRACT

80. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

81. In connection with receiving healthcare services, Plaintiff and all other Class members entered into implied contracts with Dignity, who contracted with R1.

82. Plaintiff and Class members paid money to Dignity, directly or through their insurance, and provided Dignity with their PII/PHI pursuant to said implied contracts. In exchange, Dignity agreed, and Plaintiff and Class members understood, that among other things, Dignity would: (1) provide services to Plaintiff and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (3) safeguard Plaintiff's and Class members' PII/PHI in compliance with state and federal laws, regulations, and industry standards.

83. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Dignity, on the other hand. Indeed, as set forth supra, Dignity recognized the importance of data security and the privacy of Dignity's patients' PII/PHI.

84. Had Plaintiff and Class members known that Dignity would not adequately protect their PII/PHI, they would not have agreed to provide their PII/PHI to Dignity or received healthcare or other services from Dignity, which they were required to pay for, and Dignity received compensation for in return.

85. Plaintiff and Class members performed their obligations under the implied contract when they provided Dignity with their PII/PHI and paid for healthcare or other services from Dignity.

86. Dignity breached its implied contracts with Plaintiff and the Class members in

failing to implement and maintain reasonable security measures to protect and safeguard their PII/PHI, including by ensuring companies it contracts with implement and maintain reasonable security measures to protect PII/PHI, and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner complying with applicable state and federal laws, regulations, and industry standards.

87. Dignity's breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

88. Plaintiff and all other Class members were damaged by Dignity's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) overpayment for services that were received without adequate data security.

COUNT III

UNJUST ENRICHMENT

89. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

90. Defendants received a monetary benefit from Plaintiff and the Class members in the form of monies paid to Dignity for healthcare services, which Dignity used in turn to pay for R1's services, and which was centered around Plaintiff and the Class members providing their PII/PHI in order to receive such healthcare services.

91. Defendants accepted and/or had knowledge of the benefits conferred upon them by Plaintiff and Class members; and Defendants both benefitted from the receipt of Plaintiff's and

Class members' PII/PHI, as it was used during R1's services provided to Dignity.

92. As a result of Defendants' conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for without reasonable data privacy and security practices and procedures that they received.

93. Plaintiff and the Class members would remain injured, and Defendants would be unjustly enriched if they were permitted to retain money belonging to Plaintiff and the Class members because Defendants failed to adequately implement the data privacy and security procedures that Plaintiff and Class members paid for and that were otherwise required pursuant to state and federal laws, regulations, and industry standards.

94. Defendants should be disgorged of all unlawful proceeds received by them from Plaintiff and the Class members in light of their unlawful conduct and Data Breach caused by their inadequate data security.

95. Plaintiff and the Class members are entitled to equitable relief as they have no adequate remedy at law for their injuries suffered, and continuing to accrue, as a result of Defendants' unlawful conduct and Data Breach caused by their inadequate data security.

PRAYER FOR RELIEF

96. Plaintiff, individually and on behalf of the Class, respectfully requests that (i) this action be certified as a class action, (ii) Plaintiff be designated a representative of the Class, (iii) Plaintiff's counsel be appointed as counsel for the Class.

97. Plaintiff, individually and on behalf of the Class, further requests that upon final trial or hearing, judgment be awarded against Defendants as follows:

- actual and punitive damages to be determined by the trier of fact;
- equitable relief, including restitution, as may be appropriate;
- injunctive relief, including remedial measures to be implemented by Defendants designed to prevent such a data breach by adopting improved data security practices necessary to safeguard Plaintiff and the Class members' PII/PHI and

extended identity theft protection and credit monitoring services design o protect Plaintiff and the Class members from identity theft and fraud;

- declaratory relief, as may be appropriate;
- pre- and post-judgment interest at the applicable legal rates;
- attorneys' fees, litigation expenses, and costs of suit; and
- any such other and further relief the Court deems just and proper.

DEMAND FOR JURY TRIAL

98. Plaintiff hereby demands a jury trial on all issues so triable.

DATED this 5th day of April 2024.

Respectfully submitted,

KAZEROUNI LAW GROUP, APC

By: */s/ Mona Amini*
Mona Amini, Esq.
Gustavo Ponce, Esq.
6787 W. Tropicana Ave., Suite 250
Las Vegas, Nevada 89103

Attorneys for Plaintiff